Kaspersky Security 8.0 for Microsoft Exchange Servers

Manuel d'installation

VERSION DE L'APPLICATION: 8.0 MISE A JOUR PLANIFIEE 1

Chers utilisateurs !

Nous vous remercions d'avoir choisi notre logiciel. Nous espérons que ce manuel vous sera utile et qu'il répondra à la majorité des questions.

Ce document peut être modifié sans un avertissement préalable. La version la plus récente du manuel sera disponible sur le site de Kaspersky Lab, à l'adresse .http://www.kaspersky.fr/docs

Date d'édition du document: 24.10.2011

http://www.kaspersky.fr
http://support.kaspersky.fr

TABLE DES MATIERES

PRESENTATION DU MANUEL

Les experts de Kaspersky Lab, Ltd (ci-après, Kaspersky Lab) vous souhaitent la bienvenue ! Nous espérons que ce Guide d'installation vous aidera à réaliser la procédure d'installation, à configurer l'application et à exécuter les tâches principales de Kaspersky Security 8.0 for Microsoft Exchange Servers (ci-après, Kaspersky Security ou l'application). Ce document est destiné aux administrateurs de serveurs de messagerie Microsoft Exchange Server 2007 ou 2010 (ci-après Microsoft Exchange Server ou serveur Microsoft Exchange) qui ont choisi Kaspersky Security pour assurer la protection des serveurs de messagerie.

Ce document vise à :

- Aider l'administrateur de Microsoft Exchange Server à installer les composants de l'application sur le serveur, à activer la protection du serveur et à trouver la configuration optimale en fonction des tâches en cours ;
- Offrir un accès rapide aux réponses aux questions liées à l'installation de l'application ;
- Présenter les autres sources d'informations sur l'application et les méthodes pour obtenir une assistance technique.

DANS CETTE SECTION DE L'AIDE

DANS CE DOCUMENT

Le guide d'installation de Kaspersky Security 8.0 for Microsoft Exchange Servers contient les chapitres suivants :

- Présentation du guide (cf. page 4). Le chapitre décrit la structure du guide d'installation.
- Sources d'informations complémentaires (cf. page 6). Le chapitre décrit les différentes sources d'informations sur l'achat, l'installation ou l'utilisation de Kaspersky Security.
- Kaspersky Security 8.0 for Microsoft Exchange Servers (cf. page 8). Le chapitre décrit les principales fonctionnalités de l'application.
- Configurations logicielle et matérielle (cf. page 10). Le chapitre présente la configuration matérielle et logicielle requise par Kaspersky Security.
- Préparatifs en vue de l'installation (cf. page 11). La rubrique décrit les actions préalables à toute installation de l'application.
- Mise à jour de la version antérieure de l'application (cf. page 12). Le chapitre décrit la possibilité de réaliser une mise à jour au départ d'une version antérieure de Kaspersky Security.
- Installation de l'application (cf. page 14). Le chapitre propose des instructions pas à pas sur l'installation de l'application.
- Préparatifs pour l'utilisation. Assistant de configuration initiale (cf. page 18). Le chapitre fournit les instructions sur la configuration des principaux paramètres de l'application directement après l'installation.
- Restauration de l'application (cf. page 23). Ce chapitre propose des informations sur la manière de restaurer l'application en cas de dysfonctionnement.

- Suppression de l'application (cf. page 24). Ce chapitre décrit la procédure de suppression de l'application.

CONVENTIONS

Le texte du document contient des éléments sémantiques auxquels nous vous conseillons de prêter attention. Il s'agit d'avertissements, de conseils et d'exemples.

Des convention stylistiques sont utilisées pour mettre ces éléments en évidence. Le tableau ci-dessous reprend ces conventions ainsi que des exemples d'utilisation.

Tableau 1. Conventions

EXEMPLE DE TEXTE	DESCRIPTION DE LA CONVENTION
N'oubliez pas que...	Les avertissements sont mis en évidence en rouge dans un cadre. Les avertissements contiennent des informations sur les actions indésirables potentielles pouvant entraîner la perte d'informations ou la perturbation du fonctionnement de l'appareil nomade.
Il est conseillé d'utiliser...	Les remarques figurent dans un cadre. Les remarques peuvent contenir des conseils utiles, des recommandations, des valeurs importantes ou des cas particuliers importants dans le fonctionnement de l'application.
Exemple : ...	Les exemples sont présentés sur un fond jaune sous le titre " Exemple ".
La *mise à jour*, c'est ... L'évenement *Les bases sont dépassées* s'est produit.	Les éléments suivants sont présentés en italiques : • nouveaux termes ; • noms des états et des événements de l'application ;.
Appuyez sur la touche **ENTREE**. Appuyez sur la combinaison de touches **ALT+F4**.	Les noms des touches du clavier sont écrits en caractères majuscules gras. Deux noms de touche unis par le caractère "+" représentent une combinaison de touches. Il faut appuyer simultanément sur ces touches.
Cliquez sur le bouton **Activer**.	Les noms des éléments de l'interface de l'application, par exemple, les champs de saisie, les options du menu, les boutons, sont écrits en caractères gras.
➧ *Pour planifier une tâche, procédez comme suit :*	Les phrases d'introduction des instructions sont en italique et sont précédées de l'icône "flèche".
Dans la ligne de commande, saisissez le texte `help` Les informations suivantes s'affichent : `Indiquez la date au format JJ:MM:AA.`	Les types suivants de texte apparaissent dans un style spécial : • texte de la ligne de commande ; • texte des messages affichés sur l'écran par l'application ; • données à saisir par l'utilisateur.
`<adresse IP de votre appareil nomade>`	Les variables sont écrites entre crochets pointus. La valeur correspondant à la variable remplace cette variable, sans les parenthèses angulaires sont omises.

SOURCES D'INFORMATIONS COMPLEMENTAIRES

Si vous avez des questions sur la sélection, l'achat, l'installation ou l'utilisation de Kaspersky Security, vous pouvez obtenir la réponse rapidement.

Kaspersky Lab offre diverses sources d'informations sur l'application. Vous pouvez choisir celle qui vous convient le mieux en fonction de l'importance et de l'urgence de la question.

DANS CETTE SECTION DE L'AIDE

SOURCES D'INFORMATIONS POUR UNE RECHERCHE INDEPENDANTE

Vous pouvez consulter les sources suivantes pour obtenir des informations sur l'application :

- Page de l'application sur le site de Kaspersky Lab ;
- Page de l'application sur le site du Service d'assistance technique (dans la banque de solutions) ;
- Système d'aide électronique ;
- Documentation.

Page sur le site de Kaspersky Lab

http://www.kaspersky.fr/business_products

Cette page vous propose des informations générales sur Kaspersky Security, ses possibilité et ses particularités.

Page sur le site du Service d'assistance technique (dans la banque de solutions)

http://support.kaspersky.com/fr/exchange

Cette page regroupe des articles publiés par les experts du Service d'assistance technique.

Ces articles contiennent des renseignements utiles, des recommandations et des réponses aux questions fréquemment posées sur l'utilisation de Kaspersky Security.

Système d'aide électronique

L'aide électronique contient des informations sur la manière de configurer les composants de l'application ainsi que des indications et des recommandations sur l'administration de l'application. Pour consulter l'aide électronique, sélectionnez l'option Aid dans le menu Actions de la console d'administration.

Si vous avez une question relative à une boîte de dialogue ou à un onglet en particulier dans Kaspersky Security, vous pouvez consulter l'aide contextuelle.

Pour ouvrir l'aide contextuelle, ouvrez la boîte de dialogue ou l'onglet qui vous intéresse, puis appuyez sur la touche **F1**.

Documentation

Le guide d'installation de Kaspersky Security contient toutes les informations requises pour l'installation de l'application et il fait partie de la distribution.

DISCUSSION SUR LES LOGICIELS DE KASPERSKY LAB DANS LE FORUM EN LIGNE

Si votre question n'est pas urgente, vous pouvez en discuter avec les experts de Kaspersky Lab et d'autres utilisateurs dans notre forum à l'adresse http://forum.kaspersky.fr.

Dans le forum, vous pouvez y consulter les discussions antérieures, publier des commentaires, créer une nouvelle discussion ou lancer une recherche.

CONTACTER LE GROUPE DE PREPARATION DE LA DOCUMENTATION

Si vous avez des questions sur la documentation, si vous avez découvert des erreurs ou si vous souhaitez envoyer des commentaires sur nos guides, vous pouvez contacter le groupe de rédaction de la documentation technique.

Le lien **Envoyer un commentaire** situé dans le coin supérieur droit de la fenêtre d'aide ouvrira une fenêtre du client de messagerie électronique utilisé par défaut sur votre ordinateur. Le message vide reprendra l'adresse du groupe de rédaction (docfeedback@kaspersky.com) tandis que le texte " Kaspersky Help Feedback: Kaspersky Security " apparaîtra dans l'objet du message. Laissez l'objet tel quel et écrivez votre commentaire, puis envoyez le message.

KASPERSKY SECURITY 8.0 FOR MICROSOFT EXCHANGE SERVERS

Kaspersky Security 8.0 for Microsoft Exchange Servers est une application qui a été développée pour assurer la protection des serveurs de messagerie tournant sous Microsoft Exchange Server contre les virus, les chevaux de Troie, les vers et autres types de menaces pouvant être diffusées par courrier électronique.

Les programmes malveillants peuvent provoquer de sérieux dégâts : ils sont créés spécialement pour voler des informations, les bloquer, les modifier ou les détruire et pour perturber le fonctionnement des ordinateurs et des réseaux informatiques. Lors d'une diffusion massive, un virus peut rapidement se propager dans le réseau d'une entreprise et mettre hors service non seulement les serveurs opérationnels, mais également les ordinateurs des employés, ce qui entraîne des temps morts et des pertes. De plus, les attaques de virus entraînent des pertes de données, ce qui peut avoir un impact négatif sur votre activité commerciale et sur celle de vos partenaires.

Kaspersky Security offre une protection contre le courrier indésirable au niveau du serveur de messagerie de l'organisation, ce qui ôte aux employés la nécessité de supprimer manuellement le courrier indésirable.

DANS CETTE SECTION DE L'AIDE

FONCTIONS DE BASE

Kaspersky Security protège les boîtes aux lettres, les dossiers partagés et le flux de messagerie en transit sur Microsoft Exchange Server contre les programmes malveillants et le courrier indésirable. L'ensemble du flux de messagerie qui transite via le serveur Microsoft Exchange Server protégé est analysé.

Kaspersky Security permet de réaliser les opérations suivantes :

- Analyser le flux de messagerie entrant et sortant ainsi que les messages stockés sur Microsoft Exchange Server (y compris dans les dossiers partagés) afin de détecter d'éventuels objets malveillants. Lors de l'analyse, toutes les pièces jointes sont traitées en plus du message. En fonction des paramètres définis, l'application répare ou supprime les objets malveillants découverts et fournit à l'utilisateur toutes les informations à leur sujet.

- Filtrer les messages non sollicités (spam) hors du flux de messagerie. Le composant spécial Anti-Spam analyse le flux de messagerie à la recherche de messages non sollicités. De plus, le composant Anti-Spam permet de créer des listes noire et blanche d'adresses d'expéditeurs et il prend en charge la configuration souple de l'agressivité de la recherche des messages non sollicités.

- Créer dans la Sauvegarde des copies de sauvegarde des objets (pièces jointes ou corps du message) et des messages non sollicités avant leur réparation ou leur suppression afin de pouvoir les restaurer ultérieurement, ce qui exclut la possibilité de perdre des informations. Les copies originales peuvent être localisées aisément grâce aux filtres configurables.

- Signaler à l'expéditeur, au destinataire et à l'administrateur de la protection antivirus les messages contenant des objets malveillants.

- Tenir des journaux des événements, récolter des statistiques et créer des rapports réguliers sur le fonctionnement de l'application. L'application permet créer des rapports manuellement ou selon un horaire défini.

- Configurer les paramètres de fonctionnement de l'application en fonction du volume et des caractéristiques du flux de messagerie et notamment, définir le délai de connexion pour optimiser l'analyse.

- Mettre à jour les bases de Kaspersky Security automatiquement ou selon un horaire défini. Les serveurs FTP et HTTP de mises à jour de Kaspersky Lab sur Internet, un dossier local/de réseau contenant la sélection actuelle de mise à jour ou un serveur FTP ou HTTP défini par l'utilisateur peuvent faire office de source des mises à jour.

- Lancer une analyse programmée des anciens messages (analysés antérieurement) à la recherche de nouveaux virus. Cette analyse est exécutée en arrière-plan et n'a qu'une incidence négligeable sur les performances du serveur de messagerie.

- Offrir la protection contre les virus au niveau de l'espace de sauvegarde sur la base de la liste des espaces à protéger.

DISTRIBUTION

Vous pouvez acheter Kaspersky Security chez nos partenaires ou en ligne (par exemple, http://www.kaspersky.fr, rubrique Boutique en ligne). Kaspersky Security est proposé en tant que partie de Kaspersky Security pour serveurs de messagerie, ainsi que Kaspersky Open Space Security dans Kaspersky Enterprise Space Security et Kaspersky Total Space Security. Dès que vous aurez acheté la licence pour Kaspersky Security, vous recevrez un courrier électronique reprenant un lien pour le téléchargement de l'application depuis le site de la société ainsi que le fichier de licence pour activer la licence ou vous obtiendrez un cédérom avec la distribution de l'application. Avant de décacheter l'enveloppe contenant le CD, lisez attentivement le contrat de licence.

CONTRAT DE LICENCE

Le contrat de licence est l'accord légal conclu entre vous et Kaspersky Lab qui précise les conditions d'utilisation du logiciel que vous venez d'acquérir.

Lisez attentivement le contrat de licence !

Si vous n'acceptez pas les dispositions du contrat de licence, vous pouvez refuser d'utiliser l'application et vous serez remboursé. Dans ce cas, l'enveloppe contenant le CD ne doit en aucun cas avoir été décachetée.

L'ouverture de l'enveloppe cachetée contenant le CD d'installation implique que vous acceptez tous les termes du contrat de licence.

SERVICES POUR LES UTILISATEURS ENREGISTRES

Kaspersky Lab offre à ses utilisateurs légitimes un vaste éventail de services qui leur permettent d'accroître l'efficacité de l'utilisation de l'application.

En obtenant une licence, vous devenez un utilisateur enregistré et vous pouvez bénéficier des services suivants pendant la durée de validité de la licence :

- Mise à jour toutes les heures des bases de l'application et accès aux nouvelles versions de ce logiciel ;

- Consultation par téléphone ou courrier électronique sur des questions liées à l'installation, à la configuration et à l'exploitation du logiciel ;

- Notifications de la sortie de nouveaux logiciels de Kaspersky Lab ou de l'émergence de nouveaux virus. Ce service est offert aux utilisateurs abonnés à la lettre d'informations de Kaspersky Lab via le site du service d'assistance technique.

Aucune aide n'est octroyée pour les questions relatives au fonctionnement et à l'utilisation des systèmes d'exploitation, de logiciels tiers ou de diverses technologies.

CONFIGURATIONS LOGICIELLE ET MATERIELLE

Configuration matérielle

La configuration matérielle requise par Kaspersky Security est identique à la configuration matérielle requise par Microsoft Exchange Server. En fonction des paramètres de l'application et du mode d'exploitation de celle-ci, il faudra peut-être prévoir une quantité considérable d'espace disque pour la sauvegarde et autres dossiers de service (selon la configuration par défaut, le dossier de la sauvegarde peut occuper jusqu'à 512 Mo).

La configuration matérielle pour la console d'administration installée en même temps que l'application est la suivante :

- Processeur Intel® Pentium® 400 MHz ou supérieur (recommandé : 1 000 MHz) ;
- 256 Mo de mémoire vive disponible ;
- 500 Mo d'espace disque disponible pour l'installation de l'application.

Configuration logicielle

L'installation de Kaspersky Security requiert un des systèmes d'exploitation suivants :

- Microsoft Small Business Server 2011
- Microsoft Small Business Server 2008 Standard x64
- Microsoft Small Business Server 2008 Premium x64
- Microsoft Essential Business Server 2008 Standard x64
- Microsoft Essential Business Server 2008 Premium x64
- Microsoft Windows Server® 2008 x64 R2 Enterprise Edition Service Pack 1
- Microsoft Windows Server 2008 x64 R2 Standard Edition Service Pack 1
- Microsoft Windows Server 2008 x64 Enterprise Edition Service Pack 2
- Microsoft Windows Server 2008 x64 Standard Edition Service Pack 2
- Microsoft Windows Server 2003 x64 R2 Enterprise Edition Service Pack 2
- Microsoft Windows Server 2003 x64 R2 Standard Edition Service Pack 2
- Microsoft Windows Server 2003 x64 Enterprise Edition Service Pack 2
- Microsoft Windows Server 2003 x64 Standard Edition Service Pack 2

La configuration logicielle suivante est requise pour l'installation de Kaspersky Security :

- Microsoft Exchange Server 2007 x64 Service Pack 3 ou Microsoft Exchange Server 2010 Service Pack 1, déployé dans un des rôles suivants : serveur de transport Hub, serveur de boîte aux lettres ou serveur de transport Edge ;
- Un des SGBD suivants : Microsoft SQL Server® 2005 Express Edition, Microsoft SQL Server 2005 Standard Edition, Microsoft SQL Server 2005 Enterprise Edition, Microsoft SQL Server 2008 Express Edition, Microsoft SQL Server 2008 Standard Edition, Microsoft SQL Server 2008 Enterprise Edition, Microsoft SQL Server 2008 R2 Express Edition, Microsoft SQL Server 2008 R2 Standard Edition, Microsoft SQL Server 2008 R2 Enterprise Edition ;

- Microsoft .NET Framework 3.5 Service Pack 1.

L'installation de la console d'administration requiert un des systèmes d'exploitation suivants :

- Microsoft Small Business Server 2011
- Microsoft Small Business Server 2008 Standard
- Microsoft Small Business Server 2008 Premium
- Microsoft Essential Business Server 2008 Standard
- Microsoft Essential Business Server 2008 Premium
- Microsoft Windows Server 2008 x64 R2 Enterprise Edition Service Pack 1
- Microsoft Windows Server 2008 x64 R2 Standard Edition Service Pack 1
- Microsoft Windows Server 2008 x64 Enterprise Edition Service Pack 2
- Microsoft Windows Server 2008 x64 Standard Edition Service Pack 2
- Microsoft Windows Server 2008 Enterprise Edition Service Pack 2
- Microsoft Windows Server 2008 Standard Edition Service Pack 2
- Microsoft Windows Server 2003 x64 Service Pack 2
- Microsoft Windows Server 2003 x64 R2 Standard Edition
- Microsoft Windows Server 2003 x64 R2 Enterprise Edition
- Microsoft Windows® XP x64 Service Pack 2
- Microsoft Windows Vista® x64
- Microsoft Windows Server 2003 R2 Standard Edition
- Microsoft Windows Server 2003 R2 Enterprise Edition
- Microsoft Windows Vista
- Microsoft Windows Server 2003 Service Pack 2
- Microsoft Windows XP Service Pack 3
- Microsoft Windows 7 Professional
- Microsoft Windows 7 Professional x64
- Microsoft Windows 7 Enterprise
- Microsoft Windows 7 Enterprise x64
- Microsoft Windows 7 Ultimate
- Microsoft Windows 7 Ultimate x64

La configuration logicielle suivante est requise pour l'installation de la Console d'administration :

- Microsoft Management Console 3.0 ;
- Microsoft .NET Framework 3.5 Service Pack 1.

PREPARATIFS EN VUE DE L'INSTALLATION

L'installation de Kaspersky Security requiert les privilèges d'administrateur de domaine. De plus, il faut installer les composants obligatoires suivants :

- .Net Framework 3.5 SP1 ;
- Microsoft Management Console 3.0 ;

L'utilisation de Kaspersky Security requiert une instance de serveur SQL Microsoft SQL Server 2005 / 2008 / 2008 R2 (Standard, Express, Enterprise), installée sur un des ordinateurs du réseau. Il est possible d'installer un serveur SQL sur un ordinateur doté de Kaspersky Security. Dans le cadre de l'utilisation de Kaspersky Security, il est conseillé de réinstaller le serveur SQL.

Pour pouvoir créer une base de données sur un serveur SQL, vous devez avoir les autorisations d'accès local au système de l'ordinateur sur lequel Kaspersky Security est installé ainsi que des privilèges d'administrateur sur le serveur SQL. Si le serveur SQL se trouve sur un contrôleur de domaine, vous devez être membre du groupe Administrateurs de la société et/ou Administrateurs du domaine.

MISE A JOUR DE LA VERSION ANTERIEURE DE L'APPLICATION

Kaspersky Security prend en charge la mise à jour de la version 8.0 Critical Fix 1 jusque la version actuelle. La mise à jour des versions plus anciennes de l'application n'est pas prise en charge.

La mise à jour de l'application est impossible sur les serveurs qui fonctionnent dans une configuration avec un DAG. Sur les serveurs qui appartiennent au DAG, il faut supprimer la version précédente de l'application avant d'installer la version actuelle.

Il est vivement déconseillé de mettre à jour l'application sur des serveurs fonctionnant au sein de clusters SCC et CCR car cela complique considérablement la migration des données depuis l'ancienne version de l'application vers la nouvelle. Avant d'installer la version actuelle de l'application, il est vivement conseillé de supprimer la version précédente.

Le serveur SQL qui abrite la base de données de l'application doit être accessible durant la mise à jour. Dans le cas contraire, la mise à jour se soldera sur une erreur.

Lors de la mise à jour, les valeurs des paramètres et les données de la version antérieure de l'application sont transférées à la nouvelle version.

- La licence installée pour la version antérieure est utilisée par la nouvelle version. La date de début d'utilisation de la licence est préservée sans aucune modification.
- Les valeurs des paramètres de l'application configurés dans la version précédente sont adoptés sans modifications par les paramètres correspondant de la nouvelle version, à l'exception de la case **Utiliser UDS.** Si cette case avait été cochée, elle prendra la valeur par défaut suite à la mise à jour (décochée).
- La structure de la base de données lors de la mise à jour de l'application est également actualisée. Les données de la sauvegarde et les statistiques sont conservées.
- Les rapports terminés n'apparaissent pas dans l'interface de la nouvelle version de l'application, mais ils sont enregistrés dans le dossier des rapports. (<dossier d'installation de l'application>/data/statistics/reports).

Avant de lancer la mise à jour, quittez la console d'administration.

Pour mettre à jour Kaspersky Security jusque la version actuelle, procédez comme suit :

1. Exécutez le fichier setup_ru.exe sur l'ordinateur où se trouve la version 8.0 Mise à jour critique 1 de l'application.
2. Lancez la mise à jour de l'application en cliquant sur le lien **Kaspersky Security 8.0 for Microsoft Exchange Servers**.
3. Dans la fenêtre d'accueil de l'Assistant qui s'ouvre, cliquez sur le bouton **Installer**.

   La procédure de mise à jour de l'application se déroule automatiquement.
4. A la fin de la mise à jour, cliquez sur **Terminer** afin de fermer la fenêtre de l'Assistant d'installation de l'application.

INSTALLATION DE L'APPLICATION

Kaspersky Security contient deux composants principaux : le serveur de sécurité et la console d'administration. Le serveur de sécurité est toujours installé en même temps que la console d'administration. La console d'administration peut être installée séparément sur un autre ordinateur pour l'administration à distance du serveur de sécurité. Vous avez le choix entre quatre modes d'installation en fonction de l'architecture du serveur adoptée par votre entreprise.

- Le serveur de sécurité est installé sur l'ordinateur sur lequel Microsoft Exchange Server est déployé. La console d'administration est installée sur ce même serveur.
- Le serveur de sécurité et la console d'administration sont installés sur l'ordinateur sur lequel Microsoft Exchange Server est déployé. La console d'administration est installée sur n'importe quel ordinateur du réseau de l'entreprise pour l'administration à distance du serveur de sécurité.
- Le serveur de sécurité est installé sur la grappe de serveurs sur laquelle Microsoft Exchange Server est déployé. Dans ce cas, le serveur de sécurité et la console d'administration sont installés ensemble sur chaque nœud de la grappe.
- Le serveur de sécurité s'installe sur le cluster du groupe DAG avec Microsoft Exchange Server déployé dans celui-ci. Dans ce cas, le serveur de sécurité et la console d'administration sont installés ensemble sur chaque serveur appartenant au DAG.

Après l'installation de Kaspersky Security, il convient de redémarrer certains services de Microsoft Exchange Server. Le redémarrage des services de Microsoft Exchange Server est exécuté automatiquement sans intervention.

Le programme d'installation de Kaspersky Security se présente sous la forme d'un Assistant qui fournit les informations relatives aux actions à exécuter à chaque étape. Les boutons **Précédent** et **Suivant** permettent de naviguer entre les fenêtres (étapes) de l'installation à n'importe quelle étape. Le bouton **Annuler** permet de quitter le programme d'installation. L'installation débute après l'exécution du fichier setup_ru.exe.

DANS CETTE SECTION DE L'AIDE

ETAPE 1. INSTALLATION DES COMPOSANTS INDISPENSABLES

Au cours de cette étape, vous devez confirmer que les composants indispensables suivants sont bien installés sur l'ordinateur.

- .Net Framework 3.5 SP1. Vous pouvez installer le composant en cliquant sur le bouton **Installer .Net Framework 3.5 SP1**.

L'ordinateur doit être redémarré après l'installation de .Net Framework 3.5 SP1. La poursuite de l'installation sans le redémarrage de l'ordinateur peut entraîner des échecs pendant l'utilisation de Kaspersky Security.

- Microsoft Management Console 3.0 (MMC 3.0). Microsoft Management Console 3.0 (MMC 3.0) fait partie du système d'exploitation Microsoft Windows Server 2003 R2 et ultérieur. Pour installer l'application sur une version plus ancienne de Microsoft Windows Server, il faut réaliser la mise à jour de MMC jusqu'à la version 3.0. Pour ce faire, cliquez sur le bouton **Installer MMC 3.0**.

Pour passer à l'étape suivante de l'installation, cliquez sur le lien **Kaspersky Security 8.0 for Microsoft Exchange Servers**.

Vous pouvez également télécharger et installer le guide d'installation en cliquant sur le bouton **Guide d'installation**.

ETAPE 2. MESSAGE DE BIENVENUE ET CONTRAT DE LICENCE

La fenêtre d'accueil contient des informations sur le début de l'installation de Kaspersky Security sur votre ordinateur. Cliquez sur le bouton **Suivant** pour afficher la fenêtre contenant le texte du contrat de licence.

Le contrat de licence est conclu entre l'utilisateur de l'application et Kaspersky Lab. En cochant la case **J'accepte les dispositions du contrat de licence**, vous indiquez que vous avez lu le contrat de licence et que vous en acceptez les dispositions. Si vous n'acceptez pas les conditions du contrat de licence, vous ne pourrez pas installer Kaspersky Security.

ETAPE 3. SELECTION DU TYPE D'INSTALLATION

La fenêtre de sélection du type d'installation contient deux boutons :

- **Normale**. Si vous cliquez sur ce bouton, l'installation se poursuit avec la sélection standard de composants qui répond aux besoins de la majorité des utilisateurs. Pour la suite, cf. Etape 5.

- **Personnalisée**. Si vous cliquez sur ce bouton, vous pouvez choisir les composants de l'application que vous souhaitez installer. L'installation personnalisée est recommandée pour les utilisateurs expérimentés.

Une fois le type d'installation choisi, l'Assistant d'installation passe à l'étape suivante.

ETAPE 4. SELECTION DES COMPOSANTS DE L'APPLICATION

Si vous avez choisi l'option **Personnalisée** à l'étape suivante, le programme d'installation vous propose de choisir les composants que vous voulez installer. La sélection des composants disponibles pour l'installation varie en fonction de la présence ou non de Microsoft Exchange Server sur l'ordinateur et du rôle sous lequel il a été déployé.

Si Microsoft Exchange Server est déployé simultanément dans les rôles Serveur de boîte aux lettres et serveur de transport Hub, vous aurez le choix entre les composants de l'application suivants :

- Console d'administration ;

- Module de protection contre le courrier indésirable ;

- Antivirus pour le rôle serveur de boîtes aux lettres ;

- Antivirus pour le rôle de serveur de transport Hub ou de transport Edge.

Si Microsoft Exchange Server est déployé uniquement dans le rôle de serveur de transport Hub ou de serveur de transport Edge, vous aurez le choix entre les composants de l'application suivants :

- Console d'administration ;
- Module de protection contre le courrier indésirable ;
- Antivirus pour le rôle de serveur de transport Hub ou de transport Edge.

Si Microsoft Exchange Server est déployé uniquement dans le rôle de serveur de boîte aux lettres, vous aurez le choix entre les composants de l'application suivants :

- Console d'administration ;
- Antivirus pour le rôle serveur de boîtes aux lettres.

Dans tous les autres cas, seule la console d'administration pourra être installée.

La partie inférieure de la fenêtre reprend le chemin du dossier d'installation par défaut. Si vous souhaitez choisir un autre dossier d'installation, cliquez sur le bouton **Parcourir**. Le chemin du dossier d'enregistrement des données apparaît en-dessous. Le dossier de conservation des données contient les éléments suivants :

- Bases de l'Antivirus ;
- Bases de l'Anti-Spam ;
- Objets placés en quarantaine.

Si vous pensez que le dossier va prendre plus de place que l'espace disponible sur le disque sélectionné, vous pouvez modifier le chemin d'accès au dossier de conservation en cliquant sur **Parcourir**.

Cliquez sur **Abandon** pour annuler la sélection des composants que vous aviez réalisée et revenir à la sélection par défaut.

Cliquez sur le bouton **Disques** pour ouvrir une boîte de dialogue afin de voir si les disques locaux disposent de l'espace nécessaire pour l'installation des composants sélectionnés.

ETAPE 5. CONFIGURATION DE LA CONNEXION A MICROSOFT SQL SERVER

Cette étape correspond à la configuration des paramètres de la connexion au serveur SQL.

Configuration de la connexion à Microsoft SQL Server

Dans le champ **Nom du serveur SQL**, indiquez le nom de l'ordinateur (ou son adresse IP) et l'exemplaire du serveur SQL, par exemple MYCOMPUTER\SQLEXPRESS. Cliquez sur **Parcourir**, en regard de ce champ, pour sélectionner le serveur SQL dans ce segment du réseau.

Le champ **Nom de la base de données** permet de saisir le nom de la base de données dans laquelle les données de la Sauvegarde et les statistiques seront conservées. Si la base de données portant ce nom ne figure pas sur le serveur SQL, elle est créée.

Si vous avez l'intention d'utiliser une Sauvegarde centralisée et un référentiel centralisé pour les statistiques pour plusieurs serveurs de sécurité, le nom du serveur SQL et le nom de la base de données doivent être identiques pour tous les serveurs de sécurité. Si vous n'avez pas l'intention d'utiliser un stockage centralisé, chaque serveur de sécurité peut utiliser sa propre base de données.

Si vous déployez Kaspersky Security sur un cluster de serveurs ou dans un DAG de serveurs Microsoft Exchange, il est vivement conseillé d'utiliser une base de données unique pour tous les serveurs de sécurité.

Pour créer une base de données sur le serveur SQL, il faut sélectionner le compte utilisateur sous lequel l'opération va être exécutée. Vous avez le choix entre les options suivantes :

- **Compte utilisateur actuel**. Dans cas, c'est le compte utilisateur actuel qui sera utilisé.
- **Autre compte utilisateur**. Dans ce cas, il faut indiquer le nom et le mot de passe du compte différent du compte actuel. Pour sélectionner le compte, cliquez sur **Parcourir**.

Le service du navigateur du serveur SQL doit être lancé sur l'ordinateur où se trouve le serveur SQL. Dans le cas contraire, vous ne pourrez pas voir l'instance du serveur SQL dont vous avez besoin. Si Kaspersky Security est installé sur un serveur dont le rôle est transport Edge et qu'un serveur SQL se trouve dans le domaine, il sera impossible d'établir la connexion avec le serveur SQL. Dans ce cas, il faut utiliser une instance locale du serveur SQL.

Pour pouvoir créer une base de données sur un serveur SQL, le compte utilisateur sélectionné doit avoir les autorisations d'accès local au système de l'ordinateur sur lequel Kaspersky Security est installé ainsi que des privilèges d'administrateur sur le serveur SQL. Si le serveur SQL se trouve sur un contrôleur de domaine, ce compte doit appartenir au groupe Administrateurs de la société et/ou Administrateurs du domaine. En cas de connexion à distance au serveur SQL, il convient de confirmer que la prise en charge du protocole TCP/IP est activée dans SQL Server Configuration Manager.

Sélection du compte utilisateur pour l'utilisation du service.

Dans la fenêtre suivante, vous serez invité à sélectionner le compte utilisateur qui sera utilisé pour lancer le service de l'application et la connexion au serveur SQL. Vous avez le choix entre les options suivantes :

- **Compte utilisateur Local System**. Dans ce cas, le lancement du service de l'application et la connexion au serveur SQL sont réalisés au nom du compte utilisateur du système local.
- **Autre compte utilisateur**. Dans ce cas, il faut indiquer le nom et le mot de passe du compte utilisateur. Pour sélectionner le compte, cliquez sur **Parcourir**.

Pour pouvoir utiliser la base de données existantes, le compte utilisateur sélectionné doit posséder les autorisations d'accès suivantes :

Tableau 2. Ensemble d'autorisations pour la connexion à la base de données

ENTITE DE BASE PROTEGEE	AUTORISATION	DESCRIPTION
DATABASE	CREATE TABLE	Autorisation pour ajouter des tables à la base de données sélectionnée
DATABASE	CREATE XML SCHEMA COLLECTION	Autorisation pour créer une collection de schémas XML dans la base de données sélectionnée
SCHEMA	CONTROL	Autorisation pour contrôler le schéma dbo dans la base de données sélectionnée

En cas de création d'une base de données, l'application définit automatiquement ces autorisations d'accès du compte utilisateur sélectionné.

En cas de sélection d'un compte utilisateur d'une personne enregistrée dans le domaine, il faut ajouter ce compte au groupe de domaine Exchange View-Only Administrators. Après l'ajout, il faut relancer le service de l'application sur tous les ordinateurs où il était exécuté au nom de cet utilisateur. Ceci est indispensable pour appliquer les modifications introduites dans les groupes de domaine.

ETAPE 6. COPIE DES FICHIERS

Pour poursuivre l'installation, cliquez sur **Installer** dans la fenêtre de l'Assistant d'installation. La procédure de copie des fichiers de l'application sera lancée, ainsi que l'enregistrement des composants dans le système. La base sera créée sur le serveur SQL et certains services de Microsoft Exchange Server seront redémarrés.

Le redémarrage des services de Microsoft Exchange Server est exécuté automatiquement sans intervention.

PREPARATIFS POUR L'UTILISATION. ASSISTANT DE CONFIGURATION DE L'APPLICATION

Une fois la copie des fichiers et l'enregistrement des composants dans le système terminés, l'Assistant d'installation affiche un message qui indique que l'installation est terminée. Cliquez sur **Suivant** dans l'Assistant d'installation afin d'accéder à l'Assistant de configuration de l'application. L'Assistant de configuration de l'application vous aidera à installer la licence, à configurer les paramètres de la protection, à sélectionner le mode de réception des notifications et à vérifier le fonctionnement de l'application. Pour commencer la configuration à l'aide de l'Assistant de configuration de l'application, cliquez sur **Suivant**.

DANS CETTE SECTION DE L'AIDE

INSTALLATION D'UNE LICENCE

La fenêtre **Licence** de l'Assistant de configuration de l'application permet d'installer la licence de Kaspersky Security.

Si vous déployez Kaspersky Security sur un DAG de serveurs Microsoft Exchange, il suffit d'installer la licence une fois, lors de l'installation de l'application sur n'importe lequel des serveurs du DAG. Ensuite, lors de l'installation de l'application sur d'autres serveurs du DAG, l'Assistant de configuration détectera automatiquement la licence installée. Dans ce cas, il n'est pas nécessaire d'installer à nouveau la licence.

- *Pour installer la licence, procédez comme suit :*

  1. Cliquez sur le bouton **Ajouter**.
  2. Dans la fenêtre qui s'ouvre, indiquez dans le champ **Nom du fichier** le chemin d'accès au fichier de licence (fichier portant l'extension *.key), puis cliquez sur le bouton **Ouvrir**.

     Ceci entraîne l'installation d'une licence qui vous donne le droit d'utiliser Kaspersky Security pendant la période définie par les termes de la licence.

- *Pour supprimer une licence,*

  cliquez sur le bouton **Supprimer**.

CONFIGURATION DE LA PROTECTION DU SERVEUR

La fenêtre **Paramètres de la protection** de l'Assistant de configuration de l'application permet de configurer les paramètres de protection de l'Antivirus et de l'Anti-Spam. Par défaut, la protection de l'Antivirus et de l'Anti-Spam est activée.

Pour configurer les paramètres de protection, procédez comme suit :

1. Ne décochez pas la case **Activer la protection Antivirus** afin que la protection de l'Antivirus soit active dès après le démarrage de l'application.

2. Ne décochez pas la case **Activer la protection contre le spam** afin que la protection de l'Anti-Spam soit active dès après le démarrage de l'application.

   Si vous ne souhaitez pas que la protection de l'Antivirus ou de l'Anti-Spam fonctionne directement après le démarrage de l'application, décochez les cases correspondantes. Vous allez pouvoir activer la protection via la Console d'administration plus tard.

3. Cochez la case **Activer Enforced Anti-Spam Updates Service** si vous souhaitez bénéficier de la mise à jour rapide des bases de l'Anti-Spam. Il faut aussi assurer l'exécution des conditions suivantes nécessaires pour le fonctionnement de Enforced Anti-Spam Updates Service :

   - connexion à Internet permanente pour l'ordinateur sur lequel le Serveur de sécurité est installé.

   - mise à jour régulière des bases de l'Anti-Spam (la fréquence recommandée des mises à jour : chaque 5 minutes).

4. Ne décochez pas la case **Activer le mode de mise à jour automatique des bases** si vous souhaitez autoriser la mise à jour automatique de l'Antivirus et de l'Anti-Spam depuis les serveurs de Kaspersky Lab après le démarrage de l'application.

CONFIGURATION DES PARAMETRES DU SERVEUR PROXY

La fenêtre **Paramètres du serveur proxy** de l'Assistant de configuration de l'application permet de configurer les paramètres du serveur proxy. Ces paramètres interviennent dans la connexion de l'application aux serveurs de mises à jour lors de la mise à jour des bases, ainsi que dans la connexion aux serveurs de Kaspersky Lab pendant l'utilisation des services externes de l'Anti-Spam.

Pour configurer les paramètres du serveur proxy, procédez comme suit :

1. Afin que l'application se connecte aux serveurs de Kaspersky Lab via un serveur proxy, cochez la case **Utiliser le serveur proxy**.

2. Saisissez l'adresse du serveur proxy dans le champ **Adresse du serveur proxy**.

3. Indiquez le numéro du port du serveur proxy à l'aide du menu déroulant. Le port utilisé par défaut est **8080**.

4. Pour réaliser l'authentification sur le serveur proxy que vous avez désigné, cochez la case **Utiliser l'authentification** et saisissez les données d'authentification dans les champs **Compte utilisateur** et **Mot de passe**. Pour choisir un compte utilisateur parmi les comptes existants, cliquez sur le bouton ....

5. Si vous souhaitez que les mises à jour soient téléchargées depuis un serveur local de votre entreprise sans utiliser le serveur proxy, cochez la case **Ne pas utiliser le serveur proxy pour les adresses locales**.

CONFIGURATION DES NOTIFICATIONS

La fenêtre **Configuration des notifications** de l'Assistant de configuration permet de configurer les paramètres des notifications envoyées par courrier électronique. Grâce aux notifications, vous êtes au courant de tous les événements qui se produisent dans Kaspersky Security.

Pour configurer les paramètres des notifications, procédez comme suit :

1. Dans le champ **Adresse du service Web**, indiquez l'adresse du service Web d'envoi des messages électroniques via Microsoft Exchange Server.

   Par défaut, dans Microsoft Exchange Server, il s'agit de l'adresse :

   `https://<nom_du_serveur_accès_client>/ews/exchange.asmx`

2. Dans le champ **Compte utilisateur**, indiquez n'importe quel compte parmi les boîtes aux lettres inscrites sur Microsoft Exchange Server.

   Pour ce faire, cliquez sur le bouton **Parcourir** ou saisissez le nom du compte utilisateur manuellement.

3. Saisissez le mot de passe du compte choisi dans le champ **Mot de passe**.

4. Saisissez dans le champ **Adresse de l'administrateur** l'adresse de messagerie du destinataire de la modification, par exemple votre adresse de messagerie.

5. Cliquez sur le bouton**Test** afin d'envoyer un message d'essai.

   Si le message d'essai arrive à l'adresse de messagerie indiquée, cela signifie que l'envoi des notifications est correctement configuré.

6. Cliquez sur **Suivant** pour terminer la configuration des paramètres de l'application.

7. Cliquez sur le bouton **Terminer** dans la dernière fenêtre de l'Assistant de configuration de l'application afin de quitter l'Assistant.

   Si la case **Lancer la Console d'administration à la fin de l'Assistant de configuration de l'application** est cochée, la console d'administration sera lancée automatiquement.

CONNEXION DU SERVEUR DE SECURITE

Après l'installation de Kaspersky Security, la console d'administration se connecte automatiquement au serveur de sécurité local et celui-ci s'affiche dans l'arborescence de la console d'administration. Pour réaliser la connexion à un serveur de sécurité qui se trouve sur un ordinateur distant, il faut ajouter le service Kaspersky Security à la liste des applications de confiance du pare-feu sur l'ordinateur distant ou autoriser la connexion selon RPC.

Pour connecter un autre serveur, procédez comme suit :

1. Lancez Kaspersky Security via le menu **Démarrer→Programmes →Kaspersky Security 8.0 for Microsoft Exchange Servers →Console d'administration**.

2. Choisissez le nœud **Kaspersky Security 8.0 for Microsoft Exchange Servers** dans l'arborescence de la console.

3. Dans la fenêtre des résultats, cliquez sur le bouton **Ajouter un serveur**.

4. Dans la fenêtre qui s'ouvre, choisissez l'option **Autre ordinateur**.

5. Cliquez sur le bouton **Parcourir** et désignez le serveur que vous souhaitez connecter.

6. Cliquez sur **OK**.

VERIFICATION DU FONCTIONNEMENT DE L'APPLICATION

Une fois l'installation et la configuration de Kaspersky Security terminées, il est conseillé de vérifier l'exactitude de la configuration des paramètres et le bon fonctionnement de l'application à l'aide d'un virus d'essai et de ses modifications.

Ce virus d'essai a été développé spécialement par l'organisation EICAR (The European Institute for Computer Antivirus Research) afin de tester les logiciels antivirus. Le virus d'essai n'est pas un programme malveillant et il ne contient pas de code qui pourrait nuire à votre ordinateur. Néanmoins, la majorité des logiciels antivirus le considèrent comme un virus.

Vous pouvez télécharger le virus d'essai depuis le site officiel de l'organisation EICAR : http://www.eicar.org/anti_virus_test_file.htm.

Vérification du fonctionnement de l'Antivirus

- *Pour envoyer un message avec le virus d'essai, procédez comme suit :*

  1. Créez un message avec le virus d'essai EICAR en pièce jointe.

  2. Envoyez le message via Microsoft Exchange Server sur lequel est installé Kaspersky Security avec le serveur de sécurité activé (cf. rubrique " Connexion du serveur de sécurité " à la page 21).

  3. Vérifiez que le message remis ne contient pas de virus. En cas de découverte d'un virus sur le rôle Boîte aux lettres, le virus supprimé est remplacé par un fichier texte. En cas de découverte du virus dans le rôle transport Hub, le préfixe `Malicious object deleted` est ajouté à l'objet du message.

     Une fois le virus découvert, une notification sera envoyée à l'adresse électronique indiquée dans les paramètres des notifications (cf. rubrique " Configuration des notifications " à la page 21) de l'Assistant de configuration initiale.

- *Pour consulter le rapport relatif au virus découvert dans l'application, procédez comme suit :*

  1. Lancez Kaspersky Security via le menu **Démarrer→ Programmes →Kaspersky Security 8.0 for Microsoft Exchange Servers →Console d'administration**.

  2. Dans l'arborescence de la console située à gauche, sélectionnez le nœud correspondant au serveur via lequel le message avec le virus a été envoyé et déployez-le.

  3. Sélectionnez le nœud **Rapports**.

  4. Dans le groupe de paramètres **Rapports rapides** de la fenêtre des résultats, réalisez les opérations suivantes :

     a. Dans la liste **Type**, choisissez le type de rapport **Antivirus pour le rôle serveur de boîtes aux lettres** ou **Antivirus pour le rôle de serveur de transport Hub** (en fonction de la configuration en place).

     b. Cliquez sur le bouton **Créer un rapport**.

  5. Dans le groupe de paramètres **Rapports disponibles**, consultez le rapport créé. Pour ce faire, double-cliquez sur le rapport pour l'ouvrir.

     Si le rapport contient les informations relatives à l'infection par le virus EICAR, cela signifie que les paramètres de fonctionnement de l'application ont bien été configurés.

- *Pour recevoir le rapport à l'adresse électronique, procédez comme suit :*

  1. Dans le groupe de paramètres **Rapport antivirus pour la boîte aux lettres** et **Rapport antivirus pour le rôle de serveur de transport Hub** de la fenêtre des résultats, cochez les cases **Administrateurs** pour envoyer les messages à l'adresse de messagerie que vous avez renseignée dans les paramètres des notifications (cf. section " Configuration des notifications " à la page 21) de l'Assistant de configuration de l'application.

Si vous n'aviez pas indiqué une adresse de messagerie, cliquez sur le lien **Paramètres d'envoi des messages** dans l'Assistant de configuration de l'application et configurez les paramètres d'envoi des notifications (cf. section " Configuration des notifications " à la page 21).

2. Pour confirmer que le message arrivera bien à l'adresse de messagerie électronique saisie, cliquez sur le bouton **Test** afin d'envoyer un message d'essai.

Par défaut, une copie de l'objet infecté est conservée dans la sauvegarde.

- *Pour voir si une copie de l'objet infecté a été créée dans la sauvegarde, procédez comme suit :*

1. Dans l'arborescence de la console, déployez le nœud **Sauvegarde**.

2. Confirmez que l'objet infecté (message avec virus en pièce jointe) apparaît dans la fenêtre des résultats.

Vérification du fonctionnement de l'Anti-Spam

- *Pour vérifier le fonctionnement de l'Anti-Spam, procédez comme suit :*

1. Lancez Kaspersky Security via le menu **Démarrer→Programmes →Kaspersky Security 8.0 for Microsoft Exchange Servers →Console d'administration**.

2. Dans l'arborescence de la console située à gauche, sélectionnez le nœud correspondant au serveur via lequel le message d'essai a été envoyé et déployez-le.

3. Sélectionnez le nœud **Protection du serveur**.

4. Dans la fenêtre des résultats, sélectionnez l'onglet **Protection pour le rôle serveur de transport Hub**.

5. Déployez le groupe **Paramètres des listes blanche et noire**.

6. Cochez la case **Ajouter l'adresse de l'expéditeur à la liste noire**.

7. Saisissez l'adresse de messagerie électronique de n'importe quelle boîte aux lettres à laquelle vous avez accès.

8. Cliquez sur le bouton d'ajout  à droite du champ.

9. Déployez le groupe **Paramètres d'analyse**.

10. Dans le champ **Expéditeur interdit**, choisissez la valeur **Ignorer**.

11. Dans ce même champ, cochez la case **Ajouter un intitulé**.

12. Envoyez le message depuis la boîte aux lettres indiquée vers l'adresse de l'administrateur via le serveur de messagerie protégé.

    Si le message arrive avec l'intitulé **[Blacklisted]** dans l'en-tête, l'Anti-Spam fonctionne correctement.

RESTAURATION DE L'APPLICATION

En cas d'échec du fonctionnement de l'application (par exemple, les modules exécutables sont endommagés), vous pouvez utiliser la fonction de restauration du programme d'installation. Lors de la restauration, le programme d'installation conserve les paramètres sélectionnés ainsi que les paramètres de configuration de l'utilisateur tels que les notifications ou le chemin à la base de quarantaine.

Pour restaurer Kaspersky Security, procédez comme suit :

1. Lancez le fichier setup_ru.exe.
2. Cliquez sur le lien **Kaspersky Security 8.0 for Microsoft Exchange Servers** pour ouvrir l'Assistant d'installation de l'application, puis cliquez sur le bouton **Suivant**.
3. Dans la fenêtre d'accueil de l'Assistant d'installation, cliquez sur le bouton **Suivant**.
4. Dans la fenêtre **Modification, restauration ou suppression de l'application**, cliquez sur le bouton **Restaurer**.
5. Dans la fenêtre **Restauration**, cliquez sur le bouton **Réparer**.

Si les fichiers de configuration ont été endommagés, la restauration de l'application n'est pas possible. Il est alors conseillé de supprimer l'application et de l'installer à nouveau.

SUPPRESSION DE L'APPLICATION

Pour supprimer Kaspersky Security de l'ordinateur, procédez comme suit :

1. Lancez le fichier setup_ru.exe.
2. Cliquez sur le lien **Kaspersky Security 8.0 for Microsoft Exchange Servers** pour ouvrir l'Assistant d'installation de l'application, puis cliquez sur le bouton **Suivant**.
3. Dans la fenêtre **Modification, restauration ou suppression de l'application**, cliquez sur le bouton **Supprimer**.
4. Dans la fenêtre **Suppression**, cliquez sur le bouton **Supprimer**.
5. Dans la fenêtre **Suppression de la base de données**, procédez comme suit :
   - Si vous souhaitez que la base de données soit supprimée du serveur SQL lors de la suppression de l'application, cliquez sur **Oui**.
   - Si vous souhaitez que la base de données ne soit pas supprimée du serveur SQL lors de la suppression de l'application, cliquez sur **Non**. Les données de la sauvegarde ajoutées par l'application seront supprimées de la base de données. Les statistiques ajoutées par l'application seront conservées.

Vous pouvez également supprimer l'application à l'aide des outils standard d'installation et de suppression d'applications de Microsoft Windows.

Lors de la suppression de Kaspersky Security, il faudra redémarrer certains services de Microsoft Exchange Server. Le redémarrage des services de Microsoft Exchange Server est exécuté automatiquement sans intervention.

KASPERSKY LAB ZAO

Kaspersky Lab est un éditeur de renommée mondiale spécialisé dans les systèmes de protection contre les menaces informatiques : virus et autres programmes malveillants, courrier indésirable, attaques de réseau et attaques de pirates.

En 2008, Kaspersky Lab a fait son entrée dans le Top 4 des leaders mondiaux du marché des solutions de sécurité informatique pour les utilisateurs finaux (classement " IDC Worldwide Endpoint Security Revenue by Vendor "). Selon les résultats d'une étude réalisée par KomKon TGI-Russia 2009, Kaspersky Lab est l'éditeur de système de protection préféré des utilisateurs particuliers en Russie.

Kaspersky Lab a vu le jour en Russie en 1997. Aujourd'hui, Kaspersky Lab est devenu un groupe international de sociétés dont le siège principal est basé à Moscou. La société compte cinq filiales régionales qui gèrent les activités de la société en Russie, en Europe de l'Ouest et de l'Est, au Moyen Orient, en Afrique, en Amérique du Nord et du Sud, au Japon, en Chine et dans d'autres pays de la région Asie-Pacifique. La société emploie plus de 2 000 experts qualifiés.

Produits. Les produits développés par Kaspersky Lab protègent aussi bien les ordinateurs des particuliers que les ordinateurs des réseaux d'entreprise.

La gamme de logiciels pour particuliers reprend des logiciels antivirus pour ordinateurs de bureau et ordinateurs portables ainsi que des applications pour la protection des ordinateurs de poche, des smartphones et d'autres appareils nomades.

La société propose des applications et des services pour la protection des postes de travail, des serveurs de fichiers et Internet, des passerelles de messagerie et des pare-feu. L'utilisation de ces solutions combinée à des outils d'administration centralisés permet de mettre en place et d'exploiter une protection efficace automatisée de l'organisation contre les menaces informatiques. Les logiciels de Kaspersky Lab ont obtenu les certificats des plus grands laboratoires d'essai. Ils sont compatibles avec les applications de nombreux éditeurs et sont optimisés pour de nombreuses plateformes matérielles.

Les experts de la lutte antivirus de Kaspersky Lab travaillent 24h/24. Chaque jour, ils trouvent des centaines de nouvelles menaces informatiques, développent les outils d'identification et de neutralisation de ces menaces et les ajoutent aux bases utilisées par les applications de Kaspersky Lab. *Les bases antivirus de Kaspersky Lab sont actualisées toutes les heures*, tandis que *les bases antispam* sont actualisées *toutes les 5 minutes*.

Technologies. Kaspersky Lab est à l'origine de nombreuses technologies sans lesquelles il est impossible d'imaginer un logiciel antivirus moderne. Ce n'est donc pas un hasard si le moteur logiciel de Kaspersky Anti-Virus est intégré aux logiciels de plusieurs autres éditeurs : citons notamment SafeNet (É-U), Alt-N Technologies (É-U), Blue Coat Systems (É-U), Check Point Software Technologies (Israël), Clearswift (R-U), CommuniGate Systems (É-U), Critical Path (Irlande), D-Link (Taïwan), M86 Security (É-U), GFI (Malte), IBM (É-U), Juniper Networks (É-U), LANDesk (É-U), Microsoft (É-U), NETASQ (France), NETGEAR (É-U), Parallels (Russie), SonicWALL (USA), WatchGuard Technologies (É-U), ZyXEL Communications (Taïwan). De nombreuses technologies novatrices développées par la société sont brevetées.

Réalisations. Au cours de ces années de lutte contre les menaces informatiques, Kaspersky Lab a décroché des centaines de récompenses. Ainsi, en 2010, Kaspersky Anti-Virus a obtenu plusieurs hautes distinctions Advanced+ à l'issue de tests réalisés par le célèbre laboratoire antivirus autrichien AV-Comparatives. Mais la récompense la plus importante de Kaspersky Lab, c'est la fidélité de ses utilisateurs à travers le monde. Les produits et les technologies de la société protègent plus de 300 millions d'utilisateurs. Elle compte également plus de 200 000 entreprises parmi ses clients.

Site de Kaspersky Lab	http://www.kaspersky.fr
Encyclopédie des virus	http://www.securelist.com/fr/
Laboratoire d'étude des virus	newvirus@kaspersky.com (uniquement pour l'envoi de fichiers potentiellement infectés sous forme d'archive)
	http://support.kaspersky.ru/virlab/helpdesk.html?LANG=fr
	(pour les questions aux experts antivirus)
Forum Internet de Kaspersky Lab :	http://forum.kaspersky.com

INFORMATIONS SUR LE CODE TIERS

Les informations sur le code tiers sont reprises dans le fichier legal_notices.txt situé dans le dossier d'installation de l'application.

AVIS SUR LES MARQUES

Les marques déposées et les marques de service appartiennent à leurs détenteurs respectifs.

Microsoft, Windows, Windows Server, Windows Vista, SQL Server sont des marques de Microsoft Corporation déposées aux Etats-Unis et dans d'autres pays.

Intel et Pentium sont des marques d'Intel Corporation, déposées aux Etats-Unis et dans d'autres pays.